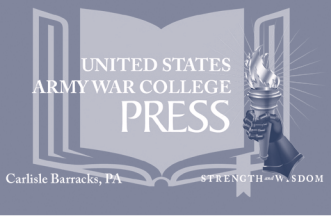
The Letort Papers



PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE

Keir Giles

Strategic Studies Institute
U.S. Army War College, Carlisle, PA

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

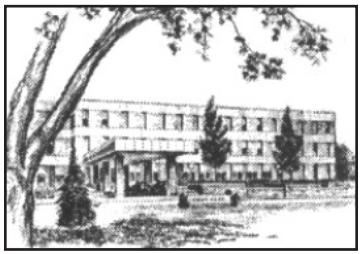
The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE

Keir Giles

January 2017

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudies Institute.army.mil*, at the Opportunities tab.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *www.StrategicStudiesInstitute.army.mil.*

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

*****

The author would like to acknowledge and extend grateful thanks to Nathalie van Raemdonck of the Belgian Federal Centre for Cyber Security for her research contributions to this Letort Paper.

ISBN 1-58487-746-4

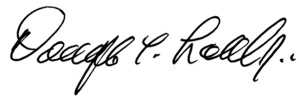
FOREWORD

At the time of this writing, the events during the 2016 presidential election campaign have focused intense attention on the dangers of hostile cyber and information operations by foreign powers. The legality under international law of this kind of interference in another state's information space has been the subject of long discussion, both bilaterally between the United States and other major cyber powers, and internationally at the United Nations (UN) and elsewhere.

In this Letort Paper, completed in late 2015, British researcher Keir Giles provides a guide to the various and conflicting trends in this debate. As a long-term scholar of the Russian approach to cyber policy and legality in cyberspace, Giles places the discussion, and U.S. concerns, in an international context. In particular, he explains the deep ideological divides on the correct course of action to take between the United States and its allies on the one hand, and a large group of nations led by Russia and China on the other.

Mr. Giles's previous work has highlighted the broad interpretation and application of "cyber power" by adversarial actors, including the potential for a range of hostile information activities that the United States would classify in entirely different domains. With this in mind, the Strategic Studies Institute recommends this Letort Paper not only to policymakers and researchers focusing on law and policy in the cyber field, but also more broadly to those engaged in protecting the United States against other forms of information operations including subversion, destabilization, and disinformation. As is shown in this Letort

Paper, legislative initiatives by potential adversaries provide important insights into the conceptual framework within which they consider and plan unfriendly actions.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

KEIR GILES is the Director of the Conflict Studies Research Centre (CSRC), a group of deep subject matter experts on Eurasian security formerly attached to the United Kingdom (UK) Ministry of Defence. Now operating in the private sector, CSRC provides in-depth analysis on a wide range of security issues affecting Russia and its relations with overseas partners.

After beginning his career working with paramilitary aviation in Russia and Ukraine immediately following the fall of the Soviet Union, Mr. Giles joined the BBC Monitoring Service (BBCM) to report on political and military affairs in the former Soviet space. While still working for the BBCM, Mr. Giles also worked for CSRC at the UK Defence Academy where he wrote and briefed for UK and North Atlantic Treaty Organization (NATO) government agencies on a wide range of Russian defense and security issues. He is an Associate Fellow of the Royal Institute of International Affairs (Chatham House) in London, UK, as well as a regular contributor to research projects on Russian security issues in both the UK and Europe. Mr. Giles's work has appeared in a wide range of academic and military publications across Europe and in the United States.

SUMMARY

This Letort Paper provides an overview of moves toward establishing international norms and the rule of law in cyberspace, and the potential for establishing further internationally accepted and enforceable standards of behavior. Completed in late 2015, it reflects the state of play in these areas at that time. It especially highlights opposing views on the nature of legality in cyberspace, and how and where those views are gaining global support.

The United States believes, in broad terms, that activities in cyberspace require no new legislation, and that existing legal obligations are sufficient. However, a large number of other states led by Russia and China believe that new international legal instruments are essential in order to govern information security overall, including as expressed through the evolving domain of cyberspace. Russia in particular argues that the challenges presented by cyberspace are too urgent to wait for customary law to develop as it has done in other domains; instead, urgent action is needed.

As well as disagreement on new legislation, there is a fundamental schism in international discussion on what exactly should constitute illegal behavior in cyberspace. Russian and Chinese information security policies express a holistic approach to countering information threats, particularly by recognizing the problem of harmful content, as well as the strict "cyber" issue of harmful code or "cyber weapons." Nevertheless, the previous basic Euro-Atlantic assumption that freedom of expression and free movement of information online are sacrosanct has now been challenged in some quarters, in the face of their exploitation by Russia and the Islamic State (IS). Hos-

tile information activities by both actors have brought clarity to the concerns over subversive content that were previously expressed by Russia and China but disavowed by the United States.

Another keystone element of the ongoing legal debate is whether, when, and to what extent the Law Of Armed Conflict (LOAC) can apply to hostile actions carried out through cyberspace, and hence the subtopic of what precisely constitutes an "armed attack" online. This Letort Paper provides an overview of the current state of the debate and progress toward international agreement, including a discussion of the *Tallinn Manual on the International Law Applicable to Cyber Warfare,* and its merits and limitations.

Further sections of this Letort Paper discuss existing rules and agreements governing cyber activity, including attempts to control cyber weapons by the Wassenaar Arrangements—an international regime regulating exports of conventional weapons and sensitive dual-use items and technologies with military end-uses—and the development of a range of international confidence building measures (CBMs) in various international organizations, including the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), the Shanghai Cooperation Organization (SCO), and more. Besides CBMs, several other codes of norms and good behavior have been constructed in regional agreements and are reviewed here, including the Council of Europe Convention on Cybercrime (the Budapest Convention). A further section discusses bilateral agreements and treaties, including those between the United States and Russia, and the United States and China.

This Letort Paper concludes with policy recommendations, including the key conclusion that adver-

saries are framing their cyber offensive potential in an entirely different mental construct than that which applies in the United States and its Western allies. The approaches of key potential state adversaries to legitimation or prohibition of online activity provides important clues to how they see this activity in terms of their own behaviors. As such, they provide a useful aid in planning for, countering, and responding to the wide range of threats to U.S. security that state and nonstate adversaries can present using the Internet.

PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE

INTRODUCTION

The application of international law and legal principles in cyberspace is a topic that has caused confusion, doubt, and interminable discussions between lawyers since the earliest days of the internationalization of the Internet. The still unresolved debate over whether cyberspace constitutes a fundamentally new domain that requires fundamentally new laws to govern it reveals basic ideological divides. On the one hand, the Euro-Atlantic community led by the United States believes, in broad terms, that activities in cyberspace require no new legislation, and existing legal obligations are sufficient. On the other, a large number of other states led by Russia and China believe that new international legal instruments are essential in order to govern information security overall, including those expressed through the evolving domain of cyberspace.[1]

Analogies for the current state of regulation in cyberspace are commonplace. The domain has been compared to the early days of highway regulations, or to maritime law. In each of these cases, the norms that were based on trust were eventually formed into customs, and were finally codified as law. Russia in particular argues that the challenges presented by cyberspace are too urgent to wait for customary law to develop as it has done in other domains; instead, urgent action is needed.

The following Letort Paper will provide an overview of moves toward establishing norms and the rule of law in cyberspace, and the potential for establishing

further international norms of behavior. It will also highlight opposing views on the nature of legality in cyberspace; and how and where those views are gaining global support.

It will be shown that despite persistent and long-term campaigning by a number of states for new binding international agreements, at present the most successful initiatives are primarily establishing norms on proper behavior through commercial interaction, and building confidence through bilateral confidence building agreements.

TO LEGISLATE, OR NOT TO LEGISLATE

Russian senior officers agree with Admiral Michael Rogers, Director of the National Security Agency (NSA) and head of U.S. Cyber Command, that deterrence in cyberspace faces serious challenges,[2] and that analogies with nuclear deterrence are flawed. However, unsurprisingly, they disagree with his proposed remedy of enhancing deterrence by increasing the United States' offensive capabilities. With escalation of cyber conflict likely, proliferation easy, and public attribution challenging, one Russian proposal is for a binding international agreement under the aegis of the United Nations (UN) that bans hostile actions in cyberspace altogether.[3]

This reflects a fundamental Russian objection to the concept of international law already applying to cyber conflict: the argument that the militarization of information space and cyber conflict should be prevented outright, rather than regulated. At the same time, Russia has also persistently proposed that technical means be developed for the recognition of facilities in cyberspace that are protected under international

humanitarian law, such as hospitals and medical facilities. Proposals range from simple top-level domains that are designated as protected, to an industry-wide set of recognized domain extensions for protective marking of validated resources, or even a simple register of Internet Protocol (IP) addresses.

In this case and others, close examination of Russian proposals often swiftly uncovers points that render them either unworkable in practice, or unacceptable to Western sensitivities.[4] Foremost among these is the assertion by Russia, China, and a wide range of other nations that content must be regulated, in addition to code.

HARMFUL CODE OR HARMFUL CONTENT

As well as disagreement on the need, or lack of a need, for new legislation, there is a fundamental schism in international discussion on what exactly ought to constitute illegal behavior in cyberspace.

Russian and Chinese information security policies express a holistic approach to countering information threats, particularly by recognizing the problem of harmful content as well as the strict "cyber" issue of harmful code.

Until very recently, Western theorists and policymakers on cyber issues were, by contrast, broadly unreceptive to the notion of harmful content. The notion that free expression of opinion constitutes a danger was seen as something wild and exotic, and rejected *a priori*, while freedom of expression and free movement of information across borders was held as sacrosanct.

This schism became clear at the World Conference on International Telecommunications (WCIT) in Dubai in December 2012. In the wake of the Arab

Spring, the Internet was perceived by Russia as a threat to domestic peace and power structures, upon which Russia actively promoted international norms to guide states' behavior in cyberspace; a call that stems from the notion that the virtual borders in cyberspace can correspond with physical state borders, thereby reaffirming the principles of sovereignty and non-intervention.[5] Russia went to WCIT with such a security-driven Internet governance agenda, proposing a state-supervised Internet.

The extent of support for the viewpoint championed by Russia from those countries that share similar concerns about the cyberthreat took the Euro-Atlantic consensus by surprise. Although Russian initiatives have been mostly discounted or ignored in the West, this is not their only audience, and Russia has been busy gathering support from countries not usually considered cyber powers, but that have a perfectly valid vote in fora such as the International Telecommunication Union (ITU) or the UN itself. This is possible because, while many of the proposals appear counter-intuitive, outdated, unworkable or otherwise unacceptable to a Western audience, they appear comforting and reasonable in those other parts of the world that see a potential threat in the unrestricted circulation of information, including hostile and damaging information, both domestically and internationally.

When Giuseppe Abbamonte of the European Commission's Directorate General for Communications Networks, Content and Technology (DG CONNECT) stated publicly that a key part of European Union (EU) cybersecurity strategy is: "**engaging with third parties and making sure that we export our values** [emphasis added]," many of those hearing him would not have taken into account that there are substan-

tial parts of the world that do not wish to have their values exported to them from Brussels[6]—and in fact, precisely this kind of export is construed as a direct information security threat in Russia's Information Security Doctrine.[7]

UKRAINE AND ISLAMIC STATE (IS)

The basic U.S. and Western assumption that freedom of expression and free movement of information online are untouchable has now been questioned, in the face of two distinct challenges to Western societies: Russian information war activities centered around the conflict in Ukraine; and the Islamic State (IS), with its own specific aims.

In both cases, a key element of the challenge is subversive disinformation and propaganda produced by "a multi-tiered online media operation in which a number of production units . . . produce content consistent with the core . . . message."[8] The result of both is that, for the first time in generations, the West has been forced to reconsider the application of the liberal principles of freedom of expression in a practical applied context—not on the basis of idealism, but in dealing with a problem that is real and immediate.

In the case of Russia, cyber activities in the broad sense are critical to offensive disinformation campaigns, whether establishing sources for disinformation by setting up false media outlets online,[9] or using social media to address targets of opportunity for subversion and destabilization efforts apparently unrelated to events in Ukraine.[10] These activities are augmented by the ubiquitous activities of trolls and bots that exploit specific features of the relationship between traditional and social media in order to both

plant, disseminate, and lend credibility to disinformation.[11] They combine for effect with a broad range of other measures, such as Russian propaganda outlets being coy about their affiliation in order to seduce viewers in the United States and elsewhere,[12] links with far-right political parties to garner direct political influence,[13] and old-school subversive measures such as: "NGO [nongovernmental organization] diplomacy, or establishing and assisting pro-Russian youth groups, minority and separatist organizations, and think tanks abroad."[14] The result is that externally, the multiplicity of deceptive narratives put forward by Russian information campaigns find fertile ground among populations that are not well informed on the realities of history, geography, and the issues at stake in Ukraine.

IS's active social media presence has prompted private companies like Twitter to take down social media accounts and block hashtags. These moves have received broad popular support, but have also been criticized by online freedom advocacy groups such as the Electronic Frontier Foundation. Twitter and similar corporations are accused of opacity on their policy of taking terrorist content offline, including the reporting threshold for triggering removal, and whether they themselves are actively searching for terrorist accounts—and if so, according to what criteria.[15] Facebook is criticized for not publicly releasing data on U.S. Government censorship requests.[16]

This debate continues. In March 2015, senior members of the House Foreign Affairs Committee sent a bipartisan letter to Twitter urging them to increase efforts to combat groups like the IS. "**Companies need to ensure that their social media services are not being hijacked for terrorist use** [emphasis add-

ed]."[17] The request was met with understanding, but was also countered with the argument they wish to preserve: "**the ability of users to share freely their views—including views that many people may disagree with or find abhorrent** [emphasis added]."[18] As an international company, Twitter must necessarily deal with the implication that complying with one government's request to censor all pro-IS users could lend support to another, less liberal government's requests to censor all anti-government users.

In an example of a de facto norm being outsourced to the private sector—since the U.S. Government and other countries have, in effect, delegated the task—corporations have developed their own codes of conduct for the content they will agree to host, to remove, and for their capabilities to censor objectionable content.[19] Although it has recently come to prominence, this is not a new phenomenon. It echoes early debates from the 1990s onward concerning where responsibility lies for the availability of illegal content found online: with the user, the service provider, or the state.

However, the result is that different private actors, applying different codes and standards, engaging in private forms of censorship on their own behalf have generated confusion and shown inconsistency. Google's policy directors are opposed to blanket censoring of IS content on its search engine and video platform YouTube, despite a stated desire not to become the distribution channel of terrorist ideology. Google states: **"Enforced silence is not the answer. Drowning out the harmful ideology with better messages, with reasonable messages, is the better way** [emphasis added]."[20] This too reflects a broader debate: some proponents of censorship have suggested a holistic government-initiated counterinsurgency tactic online,

by increasing censorship and marginalizing IS;[21] while others have suggested copying Chinese and Russian propaganda tactics, by saturating the web with counter narratives, and drowning IS propaganda in a sea of fake propaganda.[22] Neither approach would have appeared acceptable just a few years previously, before the threat of deliberate harmful content distribution became undeniable.

David Fidler, senior fellow of the Council on Foreign Relations, has proposed solutions that involve transparent cooperation of the U.S. Government with private companies. He suggests that the U.S. Government should publicly issue a presidential directive setting out the circumstances under which it will request that private companies take down content. He also pushes for private companies to explain their policies and subject them to review by independent experts, and for the government's Privacy and Civil Liberties Oversight Board to oversee government requests and report on them to Congress and the public.[23]

While the idea of harmful content, in the way Russia and China perceive it, is no longer outrageously unacceptable, the balance is yet to be found between developing an effective domestic counter-subversion strategy while not setting a dangerous precedent of censoring content online. If mishandled, the response to online subversion by IS and Russia could provide the means for abuse within the United States as well as other countries, to censor not just terrorist content but also dissenting opinions in the manner of authoritarian states that use an "extremist" label to censor anti-government social media accounts.

Despite the clear and growing evidence of challenges in this field, it can be assumed that the United States will not wish to follow the Chinese and Russian lead on restrictions of civil liberties.

The Law of Armed Conflict (LOAC).

A keystone element of the ongoing legal debates revolves around whether, when, and to what extent LOAC can apply to hostile actions carried out through cyberspace, and hence the sub-topic of what precisely constitutes an "armed attack" online. A wealth of informed legal commentary on this topic is available, and this Letort Paper will not replicate it. Instead, it will provide an overview of the current state of the debate and progress toward international agreement.

UNITED NATIONS GROUP OF GOVERNMENTAL EXPERTS (UNGGE)

The UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security is the only UN platform where state behavior in cyberspace is discussed. The group was also named tactically, to avoid discussion on information security versus cybersecurity. This was an essential step, since some states deliberately avoid any use of the term "information security" in official statements because of its negative associations. Even if the phrase is the most appropriate one to describe the topic under discussion, it has been sufficiently tainted by association with the regulatory stance adopted by Russia and China in particular, that it is shunned in favor of the more acceptable "cybersecurity."[24]

The proposal to establish the group came from Russia in 2003, with a remit to "study existing concepts and approaches and analyze current international legal provisions relating to various aspects of international information security."[25] Since then, the group has produced three consensus reports and con-

vened again in 2016. After years of stalemate, the 2013 report appeared to be a breakthrough, affirming a consensus that:

> International law, and in particular the UN Charter, is applicable, and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology] environment.[26]

How exactly the law applied and when, however, remained unspecified, and was the subject of further debate.

The 2015 report thus went deeper into the application of international law. It did, however, exclude the milestone from the previous report: that the UN Charter in its entirety applies in cyberspace. Specifically, the authorization of the use of force in self-defense against an "armed attack," as described by Article 51 of the UN Charter, was revoked.[27] According to James Lewis, the group's rapporteur and director of the Center for Strategic and International Studies' Strategic Technologies Program, the proposal was rejected by a bloc of nations, including Russia, China, Pakistan, Malaysia, and Belarus. The Chinese argument was apparently that they did not want to include reference to Article 51, because this would militarize cyberspace. According to Lewis, there was also an unspoken concern that the United States would use Article 51 to legitimize offensive counteraction for major breaches attributed to Chinese and Russian hackers.[28]

Accepting the applicability of LOAC, some states fear, will set the circumstances in which a state is justified in invoking its right to self-defense. However, it also risks encouraging the perception that all activity not expressly prohibited would be acceptable.[29]

On the application of international law, the 2015 UNGGE report outlines which of the principles of the UN charter and international law do apply to the use of ICTs:

- State sovereignty, jurisdiction over ICT infrastructure within their territory, and sovereign equality;
- Settlement of international disputes with peaceful means;
- Refraining from threat or use of force;
- Respect for human rights and fundamental freedom;
- Non-intervention in the internal affairs of other states;
- States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by nonstate actors to commit such acts;
- States must take responsibility for internationally wrongful acts attributable to them under international law. The indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a state may be insufficient to attribute activity; and,
- International legal principles of humanity, necessity, proportionality, and distinction are applicable to the use of ICTs.

The UNGGE did also identify voluntary, non-binding norms for responsible state behavior, to create an international code of conduct for information security:

- States should cooperate to increase stability and security in the use of ICTs and prevent ICT practices that are known to be harmful. They

should create a global culture of cybersecurity to protect critical information infrastructures (capacity building);
- States should not conduct, or support ICT activity that intentionally damages critical infrastructure;
- States should not allow their territory to be used for, or support internationally wrongful acts using ICTs;
- States should cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats;
- States should respect human rights on the Internet, and the right to privacy in the digital age, including the right to freedom of expression;
- States should ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products;
- States should seek to prevent the proliferation of malicious ICT tools; and,
- States should encourage responsible reporting of ICT vulnerabilities.

The power of the group and of these consensus reports is limited. Many of the delegate experts are not authorized to make national statements on behalf of their countries, and the reports have the status of non-binding recommendations. The UNGGE advises states to give active consideration to these recommendations, and to take them up for further development and implementation.

The 2013 report was subjected to a vote at the UN General Assembly, but the consensus required to adopt the report as a resolution was not reached. Little

further progress was made in the 2015 report, most likely because not all the countries with strong interests in the regulation of cyberspace were involved in the drafting of the report. States like India had already expressed their discontent with the report before it came out, since it was not allowed to contribute an expert for the group. This was a simple administrative decision rather than deliberate exclusion; India was too late responding to the call for nominations, as the group is composed on a first come, first served basis.

The 2015 report was drafted by 20 experts, five more than the 15 experts that participated in the 2013 report. While expanded, the group still is very small in size. This limited participation presents both a weakness and a strength of the UNGGE. The small membership allows the group to come to a consensus quickly. The participation of the powers wielding a veto in the UN Security Council, and an equal geographical distribution of participating countries, gives the consensus significance since it unites important differing opinions. However, the lack of universal involvement of all UN member states means it is not representative and thus has no legally binding power. The evolution of the work of this group to a UN committee would be a slow process.

Nevertheless, the representative sample of opinions presented within the UNGGE does provide a framework for further implementation by regional initiatives. For now, reports issued there carry no more than moral force.

TALLINN MANUAL

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is a handbook created by a group of international experts on how LOAC can be applicable in cyberspace. The manual is an initiative by the North Atlantic Treaty Organization (NATO) to offer guidelines to state legal advisors.[30]

The *Tallinn Manual* has posited that the general principles of international law do apply to cyberspace, including *jus ad bellum* and *jus in bello*. The manual's 95 rules define: state responsibility in cyber operations, applying the principle of prohibition of the use of force, the circumstances in which self-defense may be invoked, the conduct of parties during cyber hostilities, and more. The most important findings assert: "an international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations occurring between two states or more," and that "cyber operations alone might have the potential to cross the threshold of international armed conflict," although such conflict triggered solely in cyberspace has not yet occurred. In the manual, the experts confirmed that the instance of Stuxnet, a cyberattack on Iranian nuclear facilities with kinetic consequences, would have constituted a use of force, but did not reach the threshold of an armed attack. Under the manual, a cyber operation can be retaliated against in self-defense, but only if the conditions of a cyber armed attack ("use of force" resulting in serious physical injury and damage) are met.[31]

The *Tallinn Manual* was drafted by a group of lawyers representing the Euro-Atlantic consensus on law in cyberspace, and has not been widely adopted by the international community, in part because of the lack

of participation by nations from other regions of the world. This applies even to France; according to Jean-Christophe Noël, of the Policy Planning department in the French Ministry of Foreign Affairs, France is not in agreement with the provisions of the *Tallinn Manual,* since there is no concept of pre-emptive defense in French law—"the concept is too Anglo-Saxon." Instead, France is willing to promote the Shanghai Cooperation Organisation (SCO) or the Organization for Security and Co-operation in Europe (OSCE), to be discussed further in this Letort Paper.[32]

Many experts agree that the development of peacetime norms may ultimately be more important than establishing how international law applies during armed conflict. The majority of current cyber conflicts take place far beneath the level of armed conflict, and a lack of state practice on the actual use of force in cyberspace creates assumptions on how to respond without experience in actual situations.

The follow-on project, known as *Tallinn 2.0*, continues this reflection and focuses on the application of international law to cyberspace in peacetime. Originally scheduled to be published in late-2016, it will analyze the application of existing laws in the case of cyberattacks that are below the threshold of armed conflict, and address questions related to attribution and possible responses.

The creation of norms is also deemed more important, as well as producing trust through confidence building measures (CBMs). The next section of this Letort Paper explores the existing rules and ongoing development of norms.

EXISTING RULES AND AGREEMENTS

Cyber Weapons.

In December 2013, signatories of the Wassenaar Arrangements—an international regime regulating exports of conventional weapons and sensitive dual-use items and technologies with military end-uses—agreed to impose restrictions on exports of IP network surveillance systems and intrusion software in order to prevent "cyber proliferation." Restrictions were imposed, among others, on "zero-day" vulnerabilities that are purchased by governments as well as other customers for the purpose of targeted attacks.[33]

In July 2015, the U.S. Bureau of Industry and Security (BIS) attempted to implement the Wassenaar Arrangements, proposing a broader set of controls than intended in the Wassenaar text. BIS was challenged by the cybersecurity industry that had not been properly consulted on the specifics of such export controls.[34] They argued that controls on software deemed malicious can also hurt cybersecurity research, and as a consequence, make the Internet less safe. This is because the same offensive techniques that are developed to bypass existing computer security measures are also used by security researchers to highlight weaknesses in order to fix the vulnerable software. It became clear that the BIS proposal for implementation in effect, amounted to prohibiting the sharing of vulnerability research without a license.[35] The proposal was promptly withdrawn.

The EU is also proposing to implement the Wassenaar Arrangements, with reference to software, but has specified in more detail which software and for what purposes the export will be controlled.[36] Taking

into account that intrusion software and zero-day vulnerabilities can have useful and benign application, the EU installed safeguards for research purposes, preventing ethical hackers from being penalized. Its drafting process has encountered less resistance from the cybersecurity community, but it is still under scrutiny by researchers who vehemently oppose any export controls on intrusion software. The addition of human security in the EU amendments through an EU resolution shifts the policy focus to controlling software that is detrimental to human rights and freedom of expression.[37]

Confidence Building Measures (CBMs).

The development of a range of international CBMs in various international organizations, including the OSCE, the Organization of American States (OAS), the SCO, and more indicates a shared perception of threats and an affinity of threat perception. The challenge now appears to be expanding these shared CBMs beyond regional boundaries, and beyond the boundaries of groups of like-minded states.

CBMs are not legally binding rules, but they can often be just as effective in maintaining security and trust. They have practical applications, but are also the foundation for arriving at cyber norms and fostering responsible state behavior. CBMs prevent or reduce the risk of conflict by eliminating the causes of mistrust and miscalculation between states—an especially complex field, given the invisible and unverifiable nature of many preparations for hostile action in cyberspace.

This section will provide an overview of the impressive range of CBMs that have already been implemented through the work of international organizations.

The Organization for Security and Co-operation in Europe (OSCE).

The OSCE developed a groundbreaking set of 11 voluntary CBMs that were adopted in December 2013 by its 57 member states. These were:

- Exchanging views on various aspects of national and transnational threats to and in the use of ICTs;
- Facilitating cooperation among competent national bodies and exchange of information;
- Consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict;
- Sharing information on measures taken to ensure an open, interoperable, secure, and reliable Internet;
- Using the OSCE as a platform for dialogue, exchanging best practices, awareness-raising, and information on capacity-building;
- Putting in place modern and effective legislation to facilitate bilateral cooperation and information exchange between competent authorities;
- Sharing information on national organization, strategies, policies, and programs relevant to the security of, and use of, ICTs;
- Nominating a contact point to facilitate pertinent communications and dialogue;

- Providing a list of national terminology related to the security of, and in the use of, ICTs, accompanied by an explanation or definition of each term;
- Exchanging views using OSCE platforms and mechanisms to facilitate communications regarding the CBMs; and,
- Regular meetings of national experts to discuss the information exchanged and explore appropriate development of future CBMs.

More than three-quarters of OSCE participating states have already exchanged the specified information with other states, and the OSCE is observing and encouraging the voluntary implementation of the remaining CBMs. A further set of measures is being developed, with a focus on cooperative and "stability measures," whereby individual states commit to refrain from taking certain actions against each other.[38]

The UNGGE 2015 report based its recommended CBMs heavily on the 2013 OSCE voluntary measures, and in return, the next set of OSCE measures will be in line with the recommendations of the UNGGE report.

The Association of Southeast Asian Nations (ASEAN) Regional Forum.

In 2012, the Ministers of Foreign Affairs of the ASEAN tasked the ASEAN Regional Forum with the promotion of dialogue on confidence-building, stability, and risk-reduction measures among its members in ensuring cybersecurity. The ASEAN Regional Forum was also mandated to develop a work plan on ICT security, focusing on practical cooperation on CBMs. The ASEAN Regional Forum work plan, presented in

2015, proposes the establishment of an open-ended study group on CBMs. The workshops and preliminary reports that have been produced in support of that study group are reportedly also building on the OSCE set of CBMs.

The Organization of American States (OAS).

The OAS became the first regional body to adopt a cybersecurity strategy through approval of their resolution, "Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity," in 2004. This strategy encompassed a number of initiatives aimed at strengthening trust between member states. The main objectives of the Secretariat are to establish national "alert, watch, and warning" groups, creating a network of these Computer Security Incident Response Teams (CSIRTs); and to promote a culture and awareness of cybersecurity.[39]

CBMs in the OAS context have been primarily focused on cybercrime or infrastructure-protection capacity building initiatives, with the aim of preventing states from becoming a safe haven or permissive environment for cybercriminals. A working group of the OAS Committee on Hemispheric Security was tasked with the unification of the criteria for reporting confidence- and security-building measures (CSBMs), and created a consolidated list in 2009.[40]

The implementation of these measures has been delegated to the Inter-American Committee against Terrorism (CICTE), the process of the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), and the Inter-American Telecommunication Commission (CITEL).

Bilateral and Regional Agreements.

Several other codes of norms and good behavior have been constructed in bilateral and regional agreements.

Cybercrime: The Budapest Convention.

The 2001 European Convention on Cyber Crime (The Budapest Convention) is the first international treaty to address computer and Internet crime, and was explicitly intended to increase cooperation among nations. The Convention was drawn up by the Council of Europe and ratified by 39 countries. The Convention identifies certain offences against the confidentiality, integrity, and availability of computer data and systems as criminal activities. Under these offences is understood:

- Illegal access to data (when infringing security measures);
- The interception of data and interference (damaging, deletion, deterioration, alteration or suppression of computer data);
- Access, interception, and interference of systems;
- Creating devices and computer programs designed to make the above offences possible;
- Computer related fraud and forgery;
- Infringement of copyright; and,
- Offences in content, related to child pornography.

The signatory countries of the Convention are legally obliged to prevent, investigate, and prosecute all these actions. Through the Budapest Convention's

Mutual Legal Assistance (MLA) provisions, cooperation has improved and effective measures against cybercrime have been undertaken.[41] The advantages of the Convention as a means to resolve conflicts through law enforcement have been recognized outside Europe. Non-EU countries such as Australia, the Dominican Republic, Japan, Mauritius, Panama, Canada, and the United States are also signatories.

With the possibility for accession of non-EU countries to the Convention, the Convention can still grow to become a comprehensive international framework for all states. Brazil, China, and India; however, have argued that a treaty negotiated by Europe is inherently inapplicable to non-European countries, despite the fact that non-European countries are already party to the Convention, and a large proportion of international law that applies today stems from negotiations amongst Europeans.[42] Russia in particular, has long argued that the Budapest Convention is fatally flawed, as its provisions on access to foreign information systems violate state sovereignty. This claim was rejected in December 2014 by the committee that oversees the treaty.[43] Russia also argues, however, that the Convention should be replaced with "an entirely new document with worldwide application . . . since the Convention itself does not allow amendments."[44]

The counter-argument runs that an open-ended intergovernmental expert group already exists to conduct a comprehensive study on the problem of cybercrime, with the possibility of launching negotiations on a new cybercrime treaty under UN auspices, but this has so far not shown any results.[45] Furthermore, a new Treaty is unnecessary when the Budapest Convention has already been tested and approved by many countries and can be expanded to the rest of the world.

European Union (EU).

The EU Cybersecurity Strategy adopted in 2014 defines norms of behavior in cyberspace that all stakeholders should adhere to, following the same principles as core EU values. It has put forward proposals to fill legislative gaps identified in its National Infrastructure Strategy (NIS) on national capabilities, coordination in cases of incidents spanning across borders, and private sector involvement and preparedness.

On matters of international security, the EU encourages the development of CBMs in cybersecurity to increase transparency and reduce the risk of misperceptions in state behavior. The EU does not, however, support the creation of new international legal instruments for cyber issues.[46]

The North Atlantic Treaty Organization (NATO).

NATO's enhanced policy on cyber defense, endorsed by Allied defense ministers in June 2014, confirmed that international law applies in cyberspace. Therefore, Article 5 of the *North Atlantic Treaty* on collective self-defense can be invoked in case of a cyberattack with effects comparable to those of a conventional armed attack. However, Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters, has said that the Policy does not set any detailed criteria for the activation of Article 5, which would have to be decided by the Allies on a case-by-case basis.[47]

United States-Russia.

In June 2013, the United States and Russia signed the first bilateral agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern.

A hotline on cyber incidents was established as one of the components in the existing Direct Secure Communication System between the White House and the Kremlin. The exchange of technical information between the U.S. Computer Emergency Response Team and its Russian counterpart is another important agreement that is the first part of a set of CBMs.[48]

Russia views the bilateral agreements between itself and the United States, concluded in person by Presidents Obama and Putin, as far more advanced and significant than agreements with the EU, and has gone as far as to describe the agreement as a "pact on electronic non-aggression."[49]

However, the agreement on information exchange was welcomed by both sides as a mechanism for removing elements of suspicion or doubt, important to improve trust that seemingly malicious activity is in fact benign, and to increase transparency, ensuring a full understanding of one another's perspectives on defense policies.

United States-China.

In September 2015, the United States and China came to a significant bilateral agreement on cybersecurity.[50] While it was not the widely anticipated cyber arms control deal, an agreement was reached to abide by norms of behavior in cyberspace. At the time of this writing, these norms remain unspecified, but a senior

expert group is to be created in order to identify them, basing itself on the work done by the UNGGE. This would mean that norms set by the UNGGE could be implemented by two major cyber players in an adversarial relationship, which would constitute major progress toward international regulation.

The United States and China also agreed that neither country's government would conduct or knowingly support cyber enabled theft of intellectual property, with the intent of providing competitive advantages to companies or commercial sectors.

The timing of the agreement was significant, and relieved tension at a time when President Obama was preparing to impose sanctions against Chinese companies accused of intellectual theft shortly before a visit to the United States by Chinese President Xi Jinping.

The agreement also encompassed CBMs established through a "high-level joint dialogue mechanism on fighting cybercrime and related issues."[51] MLA would be improved, where both sides agreed to cooperate with requests to investigate cybercrimes and provide updates on the status and results of those investigations, collect electronic evidence, and mitigate malicious cyberactivity emanating from their territory. A hotline for the escalation of issues will be opened, which will drastically improve trust between the two powers, providing a framework for transparency.

Practical implementation appeared to follow swiftly, when a small number of hackers were arrested in China at the request of the U.S. Government within the following week.[52] As of yet, however, there is no public indication that China has curtailed its cyber espionage programs.

This deal was also mirrored in a UK-China bilateral pact a month later,[53] and could be the basis for further bilateral agreements.

Russia-China.

In May 2015, Russia and China signed a bilateral agreement on cooperation in the field of international information security.

This agreement was also dubbed a non-aggression pact, since both sides agreed to refrain from using cyberattacks against each other, protecting each other's internal sovereignty in cyberspace. They agreed to respond jointly to technologies that may have a destabilizing effect on political and socio-economic life or interfere with the internal affairs of the state.

In keeping with the title of the agreement and the security concerns of both states, the cyberthreats defined in the treaty are not just those that would be of concern to the EU and the United States, but they also include broadly defined threats such as the transmission of information that could endanger the "societal-political and social-economic systems, and spiritual, moral and cultural environment of states."[54]

Russia and China, together with a number of Central Asian states, have also submitted a proposal on an international code of conduct for information security, updated from an original proposal in 2011, that is currently circulating in the UN to be voted on in the General Assembly.[55]

The involvement of other states in the proposal is indicative of the support Russia and China enjoy for their concept of information security. Russia offers a powerful incentive and argument to those states that share Russia's information security concerns and

wish to ensure that national security is appropriately protected against threats in the information domain. By comparison, the West's offering is nebulous and idealistic, and focuses mainly on a discussion of the benefits (many of them intangible) that the Internet can bring. Comparisons of these two different models provide a classic example of hard versus soft interests.

United States-European Union (EU).

Dialogue commitments have also been made between the United States and the EU, the latest being at a security summit in March 2014. This dialogue provides a forum for strategic consultations on areas including: international cyberspace developments; promotion and protection of human rights online; and, politico-military and international security issues, such as norms of behavior in cyberspace, cybersecurity CBMs, and the application of existing international law and cybersecurity capacity building in third countries.[56]

Internet Governance.

Global Internet governance, the regulatory model that keeps the Internet operational, is a different topic from norms seeking, and is enacted in different fora. Governance depends on a multi-stakeholder model, while norms are developed on a state-to-state basis. The Internet is "owned" mostly by private organizations; its architecture comprises of intermediaries such as network operators, exchange points, search engines, hosting services, e-commerce platforms, and social media providers,[57] and it is these who contribute strongly to governance models.

Furthermore, debate on governance models should not be confused with discussion of legislation on what can be done in cyberspace. Rather than hard law and regulatory enforcement, governance is accomplished by means of voluntary compliance with technical standards, codes of conduct, and industry best practices. Nevertheless, the ideological dividing lines on how the Internet should be governed mirror those in discussions on how legislation should be made.

The Internet is mostly regulated through interconnectedness and peering agreements among Internet service providers, with the most important international governing bodies being the Internet Corporation for Assigned Names and Numbers (ICANN), and the International Telecommunication Union (ITU).

The ITU is the UN agency for ICT and is a provider of ITU law.[58] An important political confrontation over Internet governance came when the ITU organized the World Conference on International Telecommunications (WCIT) in Dubai in 2012, as mentioned earlier. The ITU was proposing new International Telecommunications Regulations (ITR) that had not been reviewed since 1988. These would have meant in effect that the Internet would suddenly be government led, under the regulatory framework of the ITU, and move away from a multi-stakeholder model.[59] As a result, a group of nations concerned about Internet freedom, and led by the United States, refused to sign the agreement on changes.[60]

At that point, the Internet was overseen by a loose grouping of organizations, mostly in the private sector, rather than by governments. At least one, ICANN, was operated under a contract from the U.S. Government. The importance of ICANN stems from the organization's work on the coordination of the Internet

systems of unique identifiers by coordination of IP addresses and the DNS, a hierarchical organization of namespace that is vital for the functioning of the Internet. This provided ammunition to those who claimed that the Internet was in fact run by the United States, so this arrangement was changed in 2014.

In March 2014, the U.S. Department of Commerce announced its intent to transfer its stewardship role over certain functions that keep the Internet running, known collectively as the Internet Assigned Numbers Authority (IANA), to the global multi-stakeholder community. The move was internationally applauded, as it addressed the contentious issue of U.S. control over ICANN. An important condition for the transition was that the control over IANA functions had to be exercised in a multi-stakeholder model, rather than a state-to-state model, and governments would not have ultimate decision-making authority. This removed the fear that the IANA transition would lead to a UN takeover.[61] NETMundial, hosted by Brazil, was the Global Multi-stakeholder Meeting on the Future of Internet Governance, where an outcome document was produced consolidating proposals for a roadmap on future Internet governance. Representatives from government, business, civil society, and academia were participants (actively present and remotely present) at this first of its kind multi-stakeholder meeting.[62]

Despite being due in September 2015, the IANA transition has still not occurred at the time of this writing, and administrative preparations are ongoing.[63]

A key argument in favor of the multi-stakeholder model for Internet governance, and against governance exercised only by states, is that this avoids mixing geopolitics and national preferences in with governance on technical issues. As the United States argued

in Dubai in 2012, the Internet should not be included in a draft interstate treaty dealing with technical matters like connecting international telephone calls, because doing so would replace the existing, bottom-up form of Internet oversight with a government-led model and hence, directly threaten Internet freedoms.[64]

Russia takes a contrary view. While Russia has begun to say that it supports a multi-stakeholder approach to Internet governance in principle, an important caveat is that this was with specific weight allocated to individual stakeholders. In critical questions, the state would have the right of veto, but other stakeholders would not. By contrast, Sarah Taylor, from the UK's Department of Culture Media and Sport, emphasized in December 2014 that a multi-stakeholder model needs protection against any single dominating interest. According to Jean-Jacques Sahel of ICANN, the key phrase is "avoiding capture"; for this purpose, the model needs to be as balanced as possible.

OUTLOOK, IMPLICATIONS AND POLICY RECOMMENDATIONS

This Letort Paper has given a brief overview of the relevant moves toward establishing norms and the rule of law in cyberspace. Even though the evolution of law is slow, the cyber domain is changing fast, and a measured approach to establishing norms is essential in order to ensure that they remain relevant in the longer term.

Is There a Need for a New Treaty?

The current trend of bilateral and regional implementation of CBMs, norm setting, and threat defining contributes to enhanced cybersecurity. However,

it does little to address fundamental mismatches of cybersecurity concepts between the Euro-Atlantic community and states such as Russia and China. While to some extent these can be addressed by the wide variations in interpretation of cyberthreats in the bilateral agreements between Russia and China, versus the agreements made with Western powers, it remains the case that the conceptual divergence fosters misapprehension and miscommunication.

In particular, the variation in interpretation of what constitutes hostile action in cyberspace gives rise to concern that a nation may consider itself to be in a state of hostilities with another, while that other is as yet unaware.[65]

Norms are the predecessors of an internationally agreed rule of law regime. Without universal norms, coming to an agreement on how to react to improper behavior is challenging. Therefore, the development of non-binding universal norms on appropriate behavior, governing those principles that are universally agreed, is the first priority. The UNGGE as a consensus building organization has a key role to play in this task.

Sovereignty and Rights.

Rules and regulations arrived at by negotiation between states can be abused by authoritarian regimes to suppress their own populations and deprive them of their privacy and other human rights. Setting obligations to follow international law also provides for state supervision and jurisdiction over domestic territory that has the potential to promote the application of sovereignty principles over the Internet. Any eventual international agreement must be drafted care-

fully with this in mind: that asking for more control over malicious activity may hand states the power to oppress citizens online.

The perception by Russia, China, and like-minded states that unrestricted flows of information and opinions—especially through social media—are a threat to security, gives rise to continuing efforts to constrain freedom of expression online. Their efforts to regulate information security, and especially to persuade other nations to support their international initiatives, are a challenge to Internet freedoms. Broadly speaking, it is essential to continue to resist the current efforts by Russia, China, and others to introduce legislation that would enforce controls on content as well as on hostile code. However, this does not mean that it would be impossible to arrive at specific agreements or CBMs that apply to specific activities online that all sides concur are unacceptable.

If it is important to the United States that freedom on the global web be protected, the United States needs to avoid both the fact and the appearance of constraining Internet freedom domestically. This leads to immediate challenges when attempting to counter subversive and hostile campaigns online, especially through social media, originating from the Islamic State in Iraq and Syria (ISIS) and Russia. One key remedy is transparency. When action is taken to censor or suppress content online, then having publicly visible political oversight and review of the steps taken are essential.

"Balkanization / Splinternet."

Allegations by Edward Snowden about the use of mass data collection by the United States, as well as their damage to U.S. and allied national security, has

also boosted the argument for sovereignty in cyberspace and the concept, embraced by Russia, China, and others, of "national information space."

The European Court of Justice Decision in September 2015 to end the "safe harbor" agreement sets an important precedent in this process. The lack of trust in U.S. companies and in the U.S. Government on the storage of European citizens' data has pushed European countries to end an agreement with the United States on data storage. A German data protection agency already called for data localization, the storage of network data, and communications within the territory, and others will probably follow suit.[66]

While the decision has been presented as positive for EU citizens, it also provides a precedent for further Balkanization of the Internet. Sovereignty and control over cyberspace can now legitimately be striven after by governments with far less democratic overview.[67]

The move toward devolution from the global Internet is not universal. In Brazil, proposed legislation to force all network data to be stored on Brazilian territory was dropped after heavy protests.[68] Companies like Google complained they would have to make expensive investments in server centers on Brazilian territory, and there was a perceived danger that other corporations would avoid business in Brazil altogether because of the cost, inadvertently restricting online freedom even more. The measures were too reminiscent of Brazil's recent authoritarian past, and were rejected.

Russia, however, has no such constraints, and is taking the opportunity to put in place human security measures and domestic legislation aimed at "preventing breaches in national information space." Data localization laws in Russia came into force on September 1, 2015.

Dealing with Cyber Threats.

For any arm of the U.S. Government, the current state of online legislation—and the attitudes to it around the world—has direct implications for the range of cyberthreats that face the United States, and how they can be addressed.

The approach of "trust but verify," which is the foundation of arms-control regimes in other domains, has virtually no applicability to cyberspace. Cyber threats include the capabilities of nonstate actors who are not bound by traditional diplomatic means of constraint. Meanwhile, events in Ukraine have shown that even state actors like Russia no longer consider themselves bound by norms of behavior that have been taken for granted in the West for several decades.

It is commonly held among legal experts working on the cyber domain that a catastrophic event is required in order to crystallize the law. It is only possible to arrive at a definition of an "armed attack," and determine for sure whether retaliation and self-defense was justified, when such action has been taken, the international community has reviewed those actions, and determined if there was a breach of international law.

In the meantime, in the current cyberthreat environment, acting based on trust alone would require a substantial leap of faith. There appears at present to be no substitute for additional insurance in the form of unarguably strong cyber capabilities, both defensive and offensive.

The *Tallinn Manual* and the UNGGE consensus provide models for the application of international law to actions in cyberspace. However, it is vital to

remember that although they may be attractive to the United States and its allies, they are not agreed upon by the entire international community and hence they should not be considered in any way binding on current or potential adversaries, either state or especially nonstate.

The approaches of key potential state adversaries to legitimation or prohibition of online activity provides important clues to how they see this activity in terms of their own behaviors. The widely varying attitudes displayed toward what is and is not legal and constrained in online behavior leads to a final vital point for the United States: That adversaries are framing their cyber offensive potential in an entirely different mental construct to that which applies in the United States and its Western allies. As demonstrated in Ukraine, the threat from Russia is an integrated one encompassing the whole of the information domain, as opposed to strictly technical interpretations of what constitutes cyber activity. It follows that considerable mental agility will continue to be required in order to plan for, counter, and respond to the very wide range of threats to U.S. security that state and nonstate adversaries can present using the Internet.

ENDNOTES

1. For extensive detail on this, see Keir Giles with Andrew Monaghan, *Legality in Cyberspace: An Adversary View*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, March 2014, available from *www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1193*.

2. Ellen Nakashima, "Cyber chief: Efforts to deter attacks against the U.S. are not working," *The Washington Post*, March 19, 2015, available from *https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-*

offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html.

3. MG Igor Nikolayevich Dylevskiy, Head of the Fifth Department of the Main Operations Directorate of the General Staff of the Armed Forces of the Russian Federation, Speech presented in Garmisch-Partenkirchen, Germany, April 20, 2015.

4. See detailed deconstruction in Keir Giles and Susan de Nîmes, eds., "Russia's 'Draft Convention on International Information Security': A Commentary," Oxford, UK: Conflict Studies Research Centre, April 2012.

5. Julien Nocetti, "Contest and conquest: Russia and global internet governance," *International Affairs*, Vol. 91, No. 1, January 2015, pp 110-130.

6. Speaking at Cyber Defence and Network Security Conference, London, UK, January 26, 2013.

7. According to the Information Security Doctrine of the Russian Federation, approved by President of the Russian Federation Vladimir Putin on September 9, 2000: "spiritual, moral, and cultural values of citizens" should be protected from outside influence.

8. "Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat," *Majority and Minority Staff Report*, Washington DC: U.S. Senate Committee on Homeland Security and Governmental Affairs, May 8, 2008, available from *www.hsgac.senate.gov//imo/media/doc/IslamistReport.pdf*.

9. Dalibor Rohac, "Cranks, Trolls, and Useful Idiots: Russia's information warriors set their sights on Central Europe," *Foreign Policy*, March 12, 2015, available from *https://foreignpolicy.com/2015/03/12/cranks-trolls-and-useful-idiots-poland-czech-republic-slovakia-russia-ukraine/*.

10. Doug Bernard, "America's Adversaries Use Baltimore Unrest to Spread Anti-US Message," *Voice of America News*, April 30, 2015, available from *www.voanews.com/articleprintview/2743166.html*.

11. Polina Tikhonova, "Russia Hacking Your News," ValueWalk, March 14, 2015, available from *www.valuewalk.com/2015/03/russia-hacking-your-news/*.

12. Jill Dougherty, "Russian TV's American Face," The Huffington Post, November 4, 2014, available from *www.huffingtonpost.com/jill-dougherty/russian-tvs-american-face_b_6060622.html*.

13. "«Черный интернационал». Как Москва кормит правые партии по всему миру" ("'The Black International.' How Moscow Feeds Right-Wing Parties All Over The World"), The Insider, November 27, 2014, available from *http://theins.ru/politika/2113*. See also: Andrew Higgins, "Waving Cash, Putin Sows E.U. Divisions in an Effort to Break Sanctions," *The New York Times*, April 6, 2015, available from *www.nytimes.com/2015/04/07/world/europe/using-cash-and-charm-putin-targets-europes-weakest-links.html?_r=0*.

14. Sinikukka Saari, "Russia's public diplomacy: soft tools with a hard edge," Border Crossing, Project of *Diplomat Magazine*, Vol. 1, Iss. 3, April 2015.

15. Jillian C. York, "Terrorists on Twitter: Attempts to silence ISIS online could backfire," *Slate*, June 25, 2014, available from *www.slate.com/articles/technology/future_tense/2014/06/isis_twitter_suspended_how_attempts_to_silence_terrorists_online_could_backfire.html*.

16. Dave Maass, "Why Facebook Failed Our Censorship Test," Electronic Frontier Foundation, June 18, 2015, available from *https://www.eff.org/deeplinks/2015/06/why-facebook-failed-our-censorship-test*.

17. Rick Gladstone, "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State," *The New York Times*, March 24, 2015, available from *www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html*.

18. *Ibid.*

19. Henry Farrell, "Censoring ISIS's online propaganda isn't working out very well," *The Washington Post*, June 18, 2015, available from *https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/06/18/censoring-isiss-online-propaganda-isnt-working-out-very-well/*.

20. Mark Sweney, "Google calls for anti-Isis push and makes YouTube propaganda pledge," *The Guardian*, June 24, 2015, available from *www.theguardian.com/media/2015/jun/24/google-youtube-anti-isis-push-inhuman-beheading-videos-censorship*.

21. Jared Cohen, "Digital Counterinsurgency: How to Marginalize the Islamic State Online," *Foreign Affairs*, Vol. 94, No. 6, November-December 2015, available from *https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency*.

22. Kalev Leetaru, "A Few Good Twitter Trolls: Why the United States needs to take a page from the Chinese and Russian playbooks when it comes to combating the Islamic State online," *Foreign Policy,* July 14, 2015, available from *foreignpolicy.com/2015/07/14/islamic-state-twitter-recruiting/*.

23. David P. Fidler, "Countering Islamic State Exploitation of the Internet: Cyber Brief," Council on Foreign Relations Report, June 2015, available from *www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644*.

24. Keir Giles, "Взгляд через кривое зеркало: Российские интересы в сфере информационной безопасности в представлении зарубежных государств" ("Distorting Mirror: Russian Information Security Interests As Viewed By Foreign States"), Seventh International Forum, "Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security," Moscow State University, April 2013, pp. 228-237.

25. United Nations (UN) General Assembly, 58th Session, "Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General," A/58/373, September 17, 2003.

26. UN General Assembly, 68th Session, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013.

27. UN General Assembly, 70th Session, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015.

28. Joseph Marks, "U.N. body agrees to U.S. norms in cyberspace," *Politico*, July 9, 2015, available from *www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900*.

29. Eneken Tikk-Ringas and Mika Kerttunen, "The Great Game of Cyber Norms," publication forthcoming.

30. For full text and background, see "Tallinn Manual Process," North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence (CCD) Centre of Excellence (COE) website, available from *https://ccdcoe.org/tallinn-manual.html*.

31. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, 2013, available from *https://issuu.com/nato_ccd_coe/docs/tallinnmanual/7?e=0/1803379.*

32. Speaking at the 13th International Information Security Research Consortium, Garmisch-Partenkirchen, Munich, Germany, April 2014.

33. "The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and Munitions List," December 4, 2013, available from *www.wassenaar.org/wp-content/uploads/2015/06/Previous/2013_OK/WA-LIST%20%2813%29%201.pdf.*

34. Nate Cardozo and Eva Galperin, "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?" Electronic Frontier Foundation, May 28, 2015, available from *https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation*.

35. *Ibid.*

36. See Section 5A2 Systems, Equipment and Components, in "ANNEXES to the Commission Delegated Regulation amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items," Brussels: The European Commission, October 12, 2015, available from *trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153894.pdf*.

37. European Parliament Committee on Foreign Affairs, Marietje Schaake, Rapporteur, "Report on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries'," June 3, 2015, available from *www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0178+0+DOC+PDF+V0//EN*.

38. Organization for Security and Co-operation in Europe (OSCE), "Panel 2: Avoiding Dissonance: A Round Table on Future Inter-Regional Collaboration," presentation at UN Institute for Disarmament Research (UNIDIR), "Cyber Stability 2015 'Regime Coherence'," Geneva, Switzerland, July 9, 2015, available from *www.unidir.ch/files/conferences/pdfs/-en-1-1033.pdf*.

39. Organization of American States (OAS), "Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," AG/RES. 2004 (XXXIV-O/04), adopted at the fourth plenary session, June 8, 2004, available from *www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm*.

40. Permanent Council of the OAS, Committee on Hemispheric Security, "List of confidence- and security-building measures," OAS website, January 15, 2009, available from *www.oas.org/csh/english/csbmlist.asp#Santiago*.

41. COE, Details of Treaty No. 185, "Convention on Cybercrime," Treaty open for signatures in Budapest, November 23, 2001, available from *conventions.coe.int/Treaty/en/Treaties/Html/185.htm*.

42. Alex Grigsby, "Coming Soon: Another Country to Ratify the Budapest Convention," Net Politics, Council on Foreign Relations, blog entry, posted December 11, 2014, available from *blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/*.

43. Cybercrime Convention Committee (T-CY), "T-CY Guidance Note # 3: Transborder Access to Data (Article 32)," Strasbourg, France: Council of Europe, December 3, 2014, available from *www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf*.

44. Sergey Mikhailovich Boyko, speaking at the International Information Security Research Consortium, Garmisch-Partenkirchen, Munich, Germany, April 2014.

45. UN Office on Drugs and Crime (UNODC), "Intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime to take place from 25 to 28 February 2013 in Vienna, Austria," UNODC News and Events webpage, January 18, 2013, available from *https://www.unodc.org/unodc/en/organized-crime/news/2013/cybercrime-study-expert-group-feb.html*.

46. High Representative of the European Union for Foreign Affairs and Security Policy and the European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels: European Commission, July 2, 2013.

47. "NATO Summit Updates Cyber Defence Policy," NATO CCD COE International Cyber Developments Review (INCYDER) Database, October 24, 2014, available from *https://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html*.

48. Office of the Press Secretary, "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security," Washington, DC: The White House, June 17, 2013, available from *https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol*.

49. Special Representative of the President of the Russian Federation on International Cooperation on Information Security, Ambassador at Large Andrey Krutskikh, speaking at the International Information Security Research Consortium, Garmisch-Partenkirchen, Germany, April 2014.

50. Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," Washington, DC: The White House, September 25, 2015, available from *https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states*.

51. *Ibid*.

52. Ellen Nakashima and Adam Goldman, "In a first, Chinese hackers are arrested at the behest of the U.S. government," *The Washington Post*, October 9, 2015, available from *https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html*.

53. Rowena Mason, "Xi Jinping state visit: UK and China sign cybersecurity pact," *The Guardian*, October 21, 2015, available from *www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron*.

54. See also: Russian analysis of this agreement: Elena Chernenko, "Будем дружить доменами" ("We Will Be Friends In Domains"), *Kommersant*, No. 79, May 7, 2014, available from *kommersant.ru/doc/2723155*.

55. "Annex to the Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," *International code of conduct for information security*, Presented to the 69th Session of the UN General Assembly, January 13, 2015, available from *https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf*.

56. "FACT SHEET: EU-US cooperation on cyber security and cyberspace," Brussels: European External Action Service, March 26, 2014, available from *www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf*.

57. The Global Commission on Internet Governance, About webpage, available from *https://www.ourinternet.org/about*.

58. Alexander Klimburg, ed., *National Cyber Security Framework Manual*, Tallinn, Estonia: NATO CCD COE Publications, 2012.

59. Eric Pfanner, "U.S. Rejects Telecommunications Treaty," *The New York Times*, December 13, 2012, available from *www.nytimes.com/2012/12/14/technology/14iht-treaty14.html?_r=0*.

60. "Conference concludes in Dubai with 89 countries having signed the updated International Telecommunication Regulations," WCIT2012 Hightlights, Iss. No. 6, December 13-14, 2012, available from *www.itu.int/osg/wcit-12/highlights/dec13-14.html#.VjWcDYR6nR1*.

61. Alex Grigsby, "The Top Five Cyber Policy Developments of 2014: The IANA Transition," Net Politics, Council on Foreign Relations, January 6, 2015, available from *blogs.cfr.org/cyber/2015/01/06/the-top-five-cyber-policy-developments-of-2014-the-iana-transition/*.

62. "NETmundial: the beginning of a process," About webpage for the Global Multistakeholder Meeting on the Future of Internet Governance, São Paulo, Brazil, April 23-24, 2014, available from *netmundial.br/about/*.

63. Arun Mohan Sukumar, "Governments v. ICANN: The Last Battle Before the IANA Transition," Net Politics, Council on Foreign Relations, October 27, 2015, available from *blogs.cfr.org/cyber/2015/10/27/governments-v-icann-the-last-battle-before-the-iana-transition/*.

64. Pfanner, "U.S. Rejects Telecommunications Treaty."

65. Explored in more detail in Giles, *Legality in Cyberspace*.

66. Matthias Bauer, "EU-US Safe Harbour and forced data localisation: lessons from Russia," EurActiv, October 18, 2015, available from *www.euractiv.com/sections/digital/eu-us-safe-harbour-and-forced-data-localisation-lessons-russia-318606*.

67. For a detailed view on this process from Russia, arguing that de facto "Balkanization" without a political declaration is already under way in many countries, see Aleksandra Kulikova, "Фрагментация интернета: о чем мы говорим и куда все движется?" ("Fragmentation of the Internet: What Are We Talking About and Where Is It All Going?"), PIR-Center, October 22, 2014, available from *http://www.pircenter.org/media/content/files/12/14140075130.pdf*.

68. Anthony Boadle, "Brazil to drop local data storage rule in Internet bill," Reuters, March 18, 2014, available from *www.reuters.com/article/2014/03/19/us-brazil-internet-idUSBREA2I03O20140319*.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

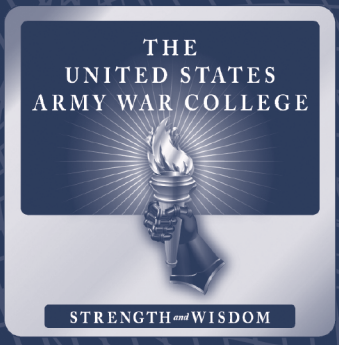
Author
Mr. Keir Giles

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil



FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

http://www.carlisle.army.mil/

ISBN 1-58487-746-4

9 781584 877462 90000>

This Publication

SSI Website

USAWC Website